Defense Threat Reduction Agency

memorandum

DATE:

REPLY TO ATTN OF:

SUBJECT:

TO:

Background: On October 26, 1999, a Defense Criminal Investigator notified (b)(6); (b)(7)(C) of the Information Assurance Division that he had received (unconfirmed) information that a DTRA computer system had been compromised. (b)(6); (b)(7)(C) immediately notified the firewall system administrator (b)(6); (b)(7)(C) Information Systems.

DTRA has, in cooperation with DISA, installed intrusion detection monitors at its 3 major locations in the Washington, DC area. On October 27, 1999 a report was generated by one of these monitors and submitted to the Information Assurance Division. SOA was again notified by the DoD-CERT of suspicious activity occurring on October 30, 1999. IS was asked to conduct a thorough examination of the system and discovered several system anomalies on November 3, 1999. Remote access to the system was turned off and all system passwords were changed.

The Chief of Staff detailed (b)(6); (b)(7)(C) to conduct an investigation on 19 November 1999. The COS further directed that (b)(6); (b)(7)(C) continue to work with the DCIS to prosecute the individual(s) involved.

Preliminary information indicated that the system was compromised on October 27, 1999. Subsequent information revealed that the system was compromised as early as August 23, 1999.

Findings: The system known as 'ns3.dtra.mil' is the backup domain name server (dns) and had been online for up to 18 months. This server is outside of the firewall (the primary domain server) and is designed to provide addressing information only. No other DTRA information is resident. There are two active system administrator accounts. A root level (total) compromise occurred with evidence suggesting the original break-in date was August 23, 1999. The intruder exploited an operating system vulnerability to originally gain access and then revised the login process so that a userid and password were not necessary to return. The preliminary Defense Criminal Investigative Service (DCIS) investigation indicated that they believe the methodology used suggests the signature of a known CONUS hacker. Discussions were held concerning chain-of-custody of the evidence and it was determined that the best approach would be for DCIS to keep the workstation in question, but provide DTRA a copy of the image tape, so that we could perform damage assessment regarding the emails which were 'captured'. (b)(6); (b)(7)(C) coordinated a joint (SOA/CI) audit review that was held at DISA headquarters on December 13/14, 1999. Together, they concluded that the email that was captured was in most cases truncated, that is 10 lines or less and predominately originated from an external user to an internal DTRA address. A substantial portion was also identified as bounced or rejected mail. SOA and CI collectively agreed that no classified information was obtained based upon their review, and that CI would provide its assessment separately.

Conclusion: (b)(6); (b)(7)(C) was asked by DCIS to provide a written report of the total costs associated with the unauthorized intrusion. A conservative figure of $5000 was provided based primarily on the expenses that the system administrators, investigators and security personnel incurred while performing analysis, damage assessments and coordination efforts. The cost of the 'downtime' and reconfiguration while the system is being held as evidence was determined to be incalculable. (b)(6); (b)(7)(C) was asked for the DIR's address so that a letter of apology could be written and was informed that the case should come to a close (a plea bargain) on or about September 21, 2000 and the evidence would be returned shortly after that.

Defense Threat Reduction Agency

memorandum

DATE: December 20, 1999

REPLY TO ATTN OF: SO, (b)(6); (b)(7)(C)

SUBJECT: Investigation into Unauthorized Access to DTRA Unclassified Computer System

TO: Chief of Staff

On October 26, 1999, a Defense Criminal Investigator notified (b)(6); (b)(7)(C) of the Information Assurance Division that he had received (unconfirmed) information that a DTRA computer system had been compromised. The investigator suggested that we take a close look at the system, identified as ns3.dtra.mil, for suspicious activity. (b)(6); (b)(7)(C) immediately notified the firewall system administrator (b)(6); (b)(7)(C) Information Systems. The Chief of Staff detailed (b)(6); (b)(7)(C) to conduct an investigation on 19 November 1999.

Incident Summary:

DTRA has, in cooperation with DISA, installed intrusion detection monitors at its 3 major locations in the Washington, DC area. On October 27, 1999 an automatic report was generated by one of these monitors, known as joint intrusion detection system (JIDS), and submitted to the Information Assurance Division. The report stated that: "multiple incorrect logins and attempts to switch user root before divulging root password in clear text occurred, and that the DoD-CERT will notify site POC of poor security practices". The system administrator was immediately notified and stated the report was correct, that she had attempted to log into ns3.dtra.mil several times because she had initially forgotten the password. IS continued to investigate the audit reports for signs of unusual activity. SO was again notified by the DoD-CERT of suspicious activity occurring on October 30, 1999. IS conducted a thorough examination of the system and discovered several system anomalies on November 3, 1999. Remote access to the system was turned off and all system passwords were changed. On the following morning, IS spoke with (b)(6); (b)(7)(C) DoD-CERT) regarding 'ns3' possibly being compromised and asked for assistance. (b)(6); (b)(7)(C) stated he would visit Tuesday morning (Nov 9) at 0630 to look at the system. He said he would also provide IS with pointers to tighten the system up. IS was asked to backup the system and provide the DoD-CERT with copies of the backup. On November 12, (b)(6); (b)(7)(C) was contacted by the DCIS and informed of the necessity of their review of the backup tapes. The tapes were secured and unavailable for delivery on that day, but arrangements were made for DCIS to pickup the unit, which was offline, on Monday November 15, 1999. A meeting was arranged to discuss the situation on November 18, 1999. A few minutes prior to the scheduled meeting, a DCIS investigator phoned (b)(6); (b)(7)(C) and reported that he was still at the DoD-CERT site and that they were still performing forensics on the system. He also stated at that time that 3 sniffer programs were found (2 active) and that up to 6500 email messages were sniffed. This information was immediately brought to the attention of (b)(6); (b)(7)(C) Chief, Information Assurance Division and Mario Vizcarra (IS), who asked that the COS be informed.

The COS asked for an immediate answer to the following questions:
Q1.) What was the time period involved?

A1.) Preliminary information indicated that the system was compromised on October 27, 1999. Subsequent information revealed that the system was compromised as early as August 23, 1999. Remote access was turned off on November 3, 1999.

Q2.) Was the classified attachment that was accidentally sent over the unclassified network in early November part of the messages that were sniffed?

A2.) The question was specifically asked of the DoD-CERT concerning email attachments. They stated that only portions of the email were sniffed, predominately header information and in some cases a few of the first lines of text. They flatly declared that no email attachments were sniffed and that it would have been impossible to do so, ASCII text was the only section of the messages that the "sniffer" program captured.

Q3.) Does the vulnerability still exist?

A3.) No, IS was asked to disable the remote access capability on all systems that are outside of the firewall and they have assured the SO that this had occurred.

Findings:

The system known as 'ns3.dtra.mil' is the backup domain name server and has been online for up to 18 months. This server is outside of the firewall (the primary domain server) and is designed to provide addressing information only. No other DTRA information is resident. There are two active system administrator accounts. A root level compromise occurred with evidence suggesting the original break-in date was August 23, 1999. The intruder exploited an operating system vulnerability to originally gain access and then revised the login process so that a userid and password were not necessary to return. The DISA-CERT notified DTRA of an increase in activity that transpired between October 27 30, 1999. An investigator from DCIS briefed IS, SO and CI on November 22, 1999. He suggested there were multiple intruders due to the fact that three separate hacker utilities were resident on the machine. The preliminary DCIS investigation indicates that they believe the methodology used suggests the signature of a known CONUS hacker. Discussions were held concerning chain-of-custody concerning the evidence and it was determined that the best approach would be for DCIS to keep the workstation in question, but provide DTRA a copy of the image tape, so that we could perform damage assessment regarding the emails which were 'sniffed'. Unfortunately, IS was unable to restore the original tape so an in-house assessment was unable to be performed. (b)(6); (b)(7)(C) coordinated a joint (SOA/CI) audit review that was held at DISA headquarters on December 13/14, 1999. They concluded that the email that was captured was in most cases truncated, that is 10 lines or less and predominately originated from an external user to an internal DTRA address. A substantial portion was also identified as bounced or rejected mail. SOA and CI collectively agreed that no classified information was obtained based upon their review, and that CI will provide it's assessment separately.

Recommendations:	**CONCUR**	**NONCONCUR**
SOA will continue to work with DCIS to prosecute the individual(s) involved. (Suspense: Ongoing)	_____	_____
IS needs to verify that all of its' external systems do not allow unencrypted remote access and that 'super user' accounts are limited to console login. (Suspense: February 24, 2000)	_____	_____
IS needs to provide SOA with a listing of all of the external IP addresses so that a vulnerability assessment (penetration test) can be thoroughly performed. (Suspense: March 24, 2000)	_____	_____
A configuration management program needs to be established as a part of the Agency's overall information assurance effort. (Suspense: IA Panel)	_____	_____
The Information Assurance Vulnerability Assessment (IAVA) process needs to be formalized and institutionalized at DTRA (see attached). (Suspense: IA Panel)	_____	_____
Install (procure) real-time monitoring tools and train those with the auditing /monitoring responsibility. (Suspense: March 24, 2000)	_____	_____
An Information Assurance (IA) emergency response, standard operating procedure (SOP) needs to be established. (Suspense: IA Panel)	_____	_____

(b)(6); (b)(7)(C)
Chief, Security Office

Attachment
as stated

MEMORANDUM FOR CHIEF, SECURITY OFFICE

SUBJECT: Report of a Security Incident, 19 November 1999

I have reviewed the subject memorandum and ( ) Concur ( ) Nonconcur with your recommendation.

FOR THE DIRECTOR:

(b)(6); (b)(7)(C)

Captain, USN
Chief of Staff

Investigator (b)(6); (b)(7)(C)
Headquarters DCIS
400 Army Navy Drive
Arlington, VA 22202-2284

Investigator (b)(6); (b)(7)(C)

As you ready this case for presentation to the USAO, I am providing you with a written report of the costs associated with the unauthorized intrusion into the system located at the Defense Threat Reduction Agency. The system known as "ns3", which provides name resolution services for the Agency, has been unavailable for many months while being held as evidence in the case. Therefore, the costs associated with the reconfiguration and the downtime experienced are incalculable at this juncture. However, Agency personnel have spent a considerable amount of time performing analysis, damage assessments as well as coordinating efforts between various Department of Defense entities that were directly caused by the intrusion. A conservative figure of $5,000 has been attributed to this case and it is primarily based upon the time devoted and salaries that were paid to the system administrators, the investigators and the security specialists who were directly involved. If you require further information, you may contact me at (b)(6); (b)(7)(C)
(b)(6);
(b)(7)(C)

(b)(6); (b)(7)(C) CISSP
Senior AIS Security
Specialist